

**DEPARTMENT OF THE NAVY
Office of the Secretary
Washington, DC 20350-1000**

**SECNAVINST 3875.1
OP-092X
2 November 1988**

SECNAV INSTRUCTION 3875.1

**From: Secretary of the Navy
To: All Ships and Stations**

**Subj: COUNTERINTELLIGENCE AND
AWARENESS BRIEFING PROGRAM**

**Ref: (a) OPNAVINST 5510.1H of 29 Apr 88
DEPARTMENT OF THE NAVY
INFORMATION AND PERSONNEL
SECURITY REGULATION**

**Encl: (1) DOD Instruction 5240.6 of
26 Feb 86**

1. Purpose. To implement enclosure (1) within the Department of the Navy (DON) as it pertains to the responsibility of the Secretary of the Navy to establish policies and procedures for the conduct of subject program. Policies and requirements specified by reference (a), the primary instruction regarding security matters with the DON, as they relate to enclosure (1) remain in effect.

2. Applicability and Scope. Reporting requirements of this instruction apply to all Department of the Navy civilian and military personnel.

3. Definitions. Terms used in this instruction are defined in enclosure (2) of enclosure (1).

4. Policy. It is Department of the Navy policy that:

a. All Department of the Navy personnel (to include all USN and USMC military personnel, active, or reserve on extended active duty, active duty for training, or inactive duty for training, all civilians, and all contractor personnel working for the Department of the Navy in any capacity) report information or circumstances which could pose a threat to the security of DON personnel, resources, facilities, or classified or controlled defense information per the requirements and procedures of reference (a).

b. All Department of the Navy personnel receive periodic briefings which address the threat posed to the Department of the Navy by hostile intelligence services and terrorist organizations and which reinforce the reporting requirements and responsibilities as specified by enclosure (1) and reference (a).

c. Appropriate judicial and administrative action shall be taken against Department of the Navy personnel who fail to report such required information.

5. Responsibilities

a. The Naval Security and Investigative Command (NSIC) is designated as the Foreign Counterintelligence (FCI) servicing agency which, on behalf of the Secretary of the Navy, provides for the conduct, direction, management, coordination, and control of subject program as it pertains to the Department of the Navy. It is the responsibility of the NSIC to collect and report to the Deputy Under Secretary of Defense for Policy the statistics and other information required by enclosure (1).

b. It is the responsibility of all Department of the Navy commands and activities, without exception, to ensure that all reports of contacts with hostile country citizens or other information relating to paragraph 4 be promptly provided to the NSIC for appropriate action.

6. Reports. The reporting requirements contained in this directive should be submitted following the requirements and procedures of reference (a).

**WILLIAM L. BALL, III
Secretary of the Navy**

**Distribution:
SNDL Parts 1 and 2
MARCORPS Codes H and I**

0579LD0540700

SECNAVINST 3875.1
2 November 1988

Commander
Naval Data Automation Command
Code 813
Washington Navy Yard
Washington, DC 20374-1662 (345 copies)

Stocked:
CO, NAVPUBFORMCEN
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (500)



Department of Defense DIRECTIVE

SECNAVINST 3875.1
2 NOV 1988

February 26, 1986#
NUMBER 5240.6

USD(P)

SUBJECT: Counterintelligence Awareness and Briefing Program

- References:
- (a) National Security Decision Directive 197, "Reporting Hostile Contacts and Security Awareness," November 1, 1985
 - (b) DoD Directive 5240.2, "DoD Counterintelligence," June 6, 1983
 - (c) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
 - (d) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
 - (e) through (j), see enclosure 1

A. PURPOSE

This Directive:

1. Implements reference (a) within the Department of Defense and reference (b) as it pertains to the responsibilities of the Deputy Under Secretary of Defense for Policy, to establish policies and procedures for the conduct and administration of DoD counterintelligence activities.
2. Establishes policy, assigns responsibilities, and prescribes procedures for reporting, investigating, and exploiting contacts by DoD personnel with citizens of communist, communist-controlled, or designated countries whose policies are inimical to the interests of the United States (see enclosure 3); and for handling other information affecting the security of DoD personnel and resources.
3. Establishes requirements for the periodic briefing of DoD personnel on hostile intelligence and terrorist threats.
4. Prescribes judicial or administrative sanctions for DoD personnel who fail to comply with the requirements of this Directive.
5. Establishes reporting requirements to the Office of the Secretary of Defense for program oversight and evaluation.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

#Reprint (7/18/86)

Enclosure (1)

2. It also applies to the extent possible to contractors participating in the Defense Industrial Security Program (reference (c)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 1.

D. POLICY

It is DoD policy that:

1. All military personnel, active and reserve (on extended active duty, active duty for training, or inactive duty for training), DoD civilian employees, and DoD contractors report to an appropriate authority information or circumstances that could pose a threat to the security of DoD personnel, resources, or classified or controlled defense information under DoD Directive 5230.24 (reference (d)) and DoD 5400.7-R (reference (e)).

2. All DoD personnel receive periodic briefings on hostile intelligence and terrorist threats, reinforcing the requirements of DoD Directive 2000.12 (reference (f)); and on their responsibility to report any such information to an appropriate authority.

3. Appropriate judicial and administrative action shall be taken when personnel fail to report such required information.

E. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy (DUSDP) shall:

a. Provide policy and direction for reporting, investigating, and exploiting reportable incidents under this Directive, pursuant to National Security Decision Directive 197 (reference (a)) and section F., below.

b. Designate one Military Department's foreign counterintelligence (FCI) agency as the Executive Agent for those DoD Components without the counterintelligence capability to implement the investigative aspects of this program.

2. The Secretaries of the Military Departments shall:

a. Provide for the conduct, direction, management, coordination, and control of this program, in accordance with this Directive.

b. Establish Military Department plans, programs, policies, and procedures to implement this program.

c. Ensure that all military and civilian personnel are periodically briefed on the requirements to report the information specified in this Directive.

d. Report annually to the OSD as outlined in subsection F.4., below.

3. The Heads of DoD Components (except Military Department Secretaries and the Director, Defense Intelligence Agency) shall:

a. Refer reported information involving military personnel assigned to their Components to the Military Department concerned for appropriate investigation and disposition; refer reported information involving civilian employees employed by their Component in the United States to their servicing DoD FCI agency and, when overseas, to the Military Department responsible for providing administrative and logistical support.

b. Establish policies and procedures to implement this program within their Components.

c. Ensure all military and civilian personnel are briefed periodically on the requirements to report the information specified in this Directive.

d. Report annually to the OSD as outlined in subsection F.4., below.

4. The Director, Defense Intelligence Agency (DIA), shall:

a. Coordinate all information reported under this Directive by military personnel assigned to DIA with the appropriate Military Department foreign counterintelligence agency; coordinate all information reported by civilian employees with the Federal Bureau of Investigation (FBI), in accordance with the Joint Agreement (reference (g)); and coordinate internal DIA investigations which uncover evidence that might lead to the arrest or prosecution of a DIA employee with the FBI or a Military Department FCI agency, as appropriate.

b. Establish policies and procedures to implement this Directive within DIA, OJCS, and the headquarters elements of U.S. Unified Commands.

c. Develop for DIA and OJCS a briefing program on security, hostile intelligence, and terrorism threat awareness.

d. Report annually to OSD as required in subsection F.4., below.

5. The Director, Defense Investigative Service (DIS), shall, in addition to the responsibilities outlined in paragraph E.3., above, develop appropriate changes to DoD 5220.22-M (reference (h)) to implement this Directive. Proposed changes shall be referred to the Office of the Deputy Under Secretary of Defense for Policy (ODUSD(P)) for preliminary policy review and approval, in accordance with DoD Directive 5220.22 (reference (c)).

6. The Director, National Security Agency (NSA), shall, in addition to the responsibilities outlined in paragraphs E.3.b., c., and d., above, coordinate all information reported under this Directive by military personnel assigned to NSA with the appropriate Military Department FCI agency, and coordinate all information reported by civilian employees with the FBI.

F. PROCEDURES

1. Reporting Requirements

a. DoD personnel who have contact with personnel or establishments of communist, communist-controlled, or other designated countries (see enclosure 3); or who have information concerning actual and potential terrorism, espionage, sabotage, subversion, or the willful compromise of classified defense information are required to report that information to their security officer, supervisor, commander, or a DoD FCI agency, for appropriate action. Each DoD Component shall establish a program requiring reporting of the following information:

(1) Any contact, intentional or unintentional, with any citizen, official, office, establishment or entity of a communist, communist-controlled, or designated country. Official, work-related, social, and professional contacts must be reported under either these or separate reporting procedures, such as those pertaining to Defense Attaches. (DoD Components should identify categories with separate reporting requirements.)

(2) Information concerning any international or domestic terrorist organization, sabotage, or subversive activity that is reasonably believed to pose or have a potential to pose a direct threat to DoD or other U.S. facilities, activities, personnel, or resources.

(3) A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or controlled defense information.

(4) Any contact with an individual (regardless of nationality) under circumstances which suggest the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

(5) Information indicating the deliberate compromise of classified defense information, attempted or contemplated by DoD personnel, with the intention of conveying classified documents, information, or material to any unauthorized persons.

b. In addition to the reporting requirements outlined above, military personnel and civilian employees are required to notify their commanders or supervisors (as appropriate) before contacting or visiting any establishment of a communist, communist-controlled, or designated country (see enclosure 3), including those located within the United States and friendly countries, whether for private or official reasons. (NOTE: Military personnel must obtain their commander's approval before visiting such establishments/entities.) Subsequent to any such visit or contact, the reporting requirement of subparagraph F.1.a.(1), above, shall apply.

c. All DoD personnel shall receive periodic briefings on hostile intelligence and terrorist threats and be advised of their personal responsibility to report information, in accordance with paragraphs F.1.a. and b., above.

2. Sanctions

Any DoD personnel who fail to report information required by this Directive shall be subject to judicial (Uniform Code of Military Justice - UCMJ) or administrative action appropriate to the seriousness of the offense.

3. Analysis of Reports

For purposes of analysis and uniformity of reporting among DoD Components, the following categories and subcategories shall be used for reports made under this Directive:

- a. CATEGORY I. Includes any reported incident of an approach or request for information in which hostile intelligence service involvement is confirmed.
- b. CATEGORY II. Includes any reported incident of an approach or request for information in which some evidence suggests hostile intelligence service involvement (based on the name used by the perpetrator/elicitor, physical description, modus operandi, or the nature of the information requested).
- c. CATEGORY III. Includes any reported solicitation of classified or unclassified defense information not made through official channels or under authorized procedures, in which foreign intelligence service involvement is considered to be remote.
- d. CATEGORY IV. Includes any reported incident or contact with a citizen or entity of a communist, communist-controlled, or designated country, responsive to the requirements, although available evidence indicates that foreign intelligence service involvement is unlikely.
- e. CATEGORY V. Includes any reported information concerning international or domestic terrorist groups/activities that pose a potential threat to the security of DoD or other U.S. personnel, resources, or facilities.
- f. CATEGORY VI. Includes any reported incident of deliberate compromise of classified defense information by DoD personnel to an unauthorized person or entity.

4. Reporting Requirements

For the purpose of oversight and program evaluation, DoD Components or their servicing DoD FCI agencies shall maintain a record of the incidents and information reported in each category listed in paragraphs F.3.a. through f., above. An annual report containing the following information for the preceding fiscal year shall be provided to the Director of Counterintelligence and Investigative Programs, Office of the Deputy Under Secretary of Defense for Policy, by November 1:

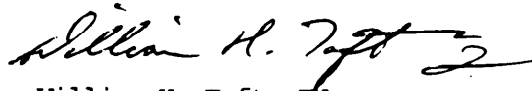
- a. Number of personnel briefed on reporting requirements.
- b. Number of contacts or reports received by category.
- c. Number of investigations initiated as a result of information reported.
- d. Number of investigations resulting in:
 - (1) Planned or actual offensive counterespionage operations.

- (2) Confirmed instances of espionage.
- (3) Confirmed deliberate compromise of defense information.
- (4) Administrative or judicial action against individuals violating reporting requirements.
- (5) Persons prosecuted or pending prosecution on charges of espionage or related offenses, based upon reports under this Directive.

e. Reports involving information on terrorist threats to the security of DoD or other U.S. personnel and resources.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Policy within 120 days.


William H. Taft, IV
Deputy Secretary of Defense

Enclosures

- 1. References
- 2. Definitions
- 3. Communist or Communist-Controlled or Designated Countries

REFERENCES, continued

- (e) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, March 24, 1980
- (f) DoD Directive 2000.12, "Protection of DoD Personnel and Resources Against Terrorist Acts," February 12, 1982
- (g) Agreement Governing the Conduct of Department of Defense Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979
- (h) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," March 1984, authorized by DoD Directive 5220.22, December 8, 1980
- (i) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
- (j) Title 18, United States Code, Sections 150, 792-798, and 2387

DEFINITIONS

1. Citizen. As used in this Directive, any communist, communist-controlled or designated country representative, diplomat, visitor, tourist, student, scholar, journalist, engineer, scientist, athlete, businessperson, or other person from a communist, communist-controlled, or designated country.
2. Classified Defense Information. Official information requiring protection in the interest of national defense, classified TOP SECRET, SECRET, or CONFIDENTIAL according to DoD 5200.1-R (reference (i)), or designated Sensitive Compartmented Information (SCI) according to DoD TS 5105.21-M2 or DoD TS 5105.21-M3.
3. Contact. Any form of meeting, association, or communication; in person, by radio, telephone, letter or other means, regardless of who initiated the contact or whether it was for social, official, private, or other reasons with a citizen or entity of a communist, communist-controlled, or designated country. A contact has occurred even if no official information was discussed or requested.
4. Controlled Information. As used in this Directive, that information which bears a distribution limitation statement from DoD Directive 5230.24 (reference (d)) or that information which is being marked "For Official Use Only" in accordance with Chapter IV of DoD 5400.7-R (reference (e)).
5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.
6. Counterintelligence Investigation. Includes inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of a foreign power for purpose of espionage or other intelligence activities, sabotage, assassinations, international terrorist activities; and actions to neutralize such acts.
7. Criminal Subversion. Criminal subversion is defined in 18 U.S.C. 2387 (reference (j)). It generally includes inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline, of the military forces of the United States.
8. Deliberate Compromise of Classified Information. Instances in which classified defense information is or could be compromised as a result of willful disclosure to an unauthorized person.
9. Entity. Any embassy; consulate; trade, press, airline, cultural, tourist, or business office; and any organization representing a communist, communist-controlled, or designated country.

10. Espionage. As set forth in 18 U.S.C. 792-798 (reference (j)), in general:

a. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace.

b. The statute makes it an offense to gather, with the requisite intent or belief, national defense information, by going upon, entering, flying over, or obtaining access by any means to any installation or place used by the United States in connection with national defense. The method of gathering information is immaterial.

c. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it, is guilty of espionage.

d. Anyone entrusted with or having lawful possession or control of information pertaining to national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of this trust, is guilty of violating the Espionage Act.

e. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of the Espionage Act.

11. Sabotage. An act or acts with the intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war material, premises, or utilities, to include human or natural resources. Such activity is a violation of 18 U.S.C. 150 (reference (j)).

12. Terrorism. The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.

COMMUNIST OR COMMUNIST-CONTROLLED OR DESIGNATED COUNTRIES

Afghanistan
Albania
Angola
Bulgaria
Cambodia (Kampuchea)
Cuba (except U.S. Naval Base, Guantanamo)
Czechoslovakia
Ethiopia
German Democratic Republic (East Germany, including the Soviet Sector of Berlin)
Hungary
Iran
Iraq
Laos
Libya
Nicaragua
North Korea (and adjacent demilitarized zone)
Outer Mongolia (Mongolian People's Republic)
Poland
People's Democratic Republic of Yemen (South Yemen)
Romania
Syria
Union of Soviet Socialist Republics (USSR)
Vietnam
Yugoslavia